

ADDITIONAL FEE:

Please charge any insufficiency of fee, or credit any excess, to Deposit Account No. 50-0427.

R E M A R K S

The Office Action issued November 19, 2002 has been received and its contents have been carefully considered.

Submitted herewith is a copy of applicant's Information Disclosure Statement, dated January 24, 2001. Apparently, the sheets of Form PTO 1449, which were included with the Statement, became separated from the U.S. PTO file.

Also enclosed herewith are copies of the formal drawings showing the changes in red ink which are included in the enclosed formal drawings. As the Examiner will see, a number of reference numerals have been added to Figs. 1 and 2; the term "Processor" in Fig. 3 was changed to -- Host Computer -- to render it consistent with Fig. 4, and the box "Processor 30" has been deleted from Fig. 5. This processor 30 has not been referred to in the specification (page 64) and is unnecessary for an understanding of the invention.

The term "stenangiographic", which appears at several places throughout the specification has been changed to "steganographic", which is the proper term.

The claims of this application have been reviewed and amended to state that the document is imprinted with document content "comprising at least one of text and graphic images" and "by means of a computer printer". These amendments clarify what was originally intended but left unsaid in the claims, and thus render the claims more clear and definite. Claim 72 has also been amended to delete the limitation that the document stock "has anticounterfeit features". This limitation has been inserted in dependent claim 77 and the limitation previously recited in claim 77 has been moved to claim 85.

The present invention relates to a system and method for producing and authenticating paper documents and their contents. It provides a counterfeit resistant paper document. This system uses several security features. For example, the document content may be summarized and encrypted with the sender's unique private key. The paper document may be authenticated at any time by checking the

security features and digital signatures. The system prevents counterfeiting of valuable paper documents by providing both physical and logical security.

Delivering authentic digital files (digital document files) via the Internet invites fraud, while delivery of paper documents via postal or other commercial delivery services is, by comparison, less efficient and time consuming. Remote printing of authentic paper documents from digital files is the logical next step to provide efficient, timely service. The present invention is intended to solve this problem.

While it is possible to verify the delivery and authenticity of the content of digital files, it has not been possible to transfer that same authenticity from the digital realm to the tangible realm of paper documents. The present invention enables this authenticity to be transferred to paper.

It is possible today to transmit a digital file over the Internet and authenticate it. Prior to the present invention, however, this authentication could not be transferred to a paper document. The contents of any

digital file can be copied with a screen capture program, modified, and printed out without disclosing the changes. The present invention assures that any alterations from the transmitted digital file are readily detected.

Independent claims 53 and 72 recite certain essential steps for producing original paper documents at remote locations. Independent claim 88 defines an authenticatable paper document itself.

For the information of the Examiner, the system for producing authenticatable, counterfeit-resistant documents is explained below:

- A paper document is preprinted with a unique identification with counterfeit-resistant features at the bottom of each page. This paper is delivered to the remote site in advance.
- The information in the digital file to be printed on each page is summarized using a digital digest and signed with the provider's secret key.
- This information is combined with the unique identification of the pre-printed page and other information needed for identification and decomposition of the signed

digital digest, using cryptography and public key infrastructure (PKI). This information is further signed with an private key.

- The resulting information from the prior step is translated into printable characters and appended to plain text identification information to form an authentication stripe.
- This authentication stripe is appended to the bottom of each page in the digital file. The file is then delivered to the remote printing site.
- A standard laser printer is used to print the content of this digital file onto paper containing the counterfeit-resistant information, to produce an authenticatable paper document.
- Each page of this paper document is counterfeit resistant and exceeds the legal requirements for a digital signature.
- A third party authenticating agent, such as a qualified law firm or bank, can independently verify that each page of the printed document was sent from the specified provider, produced at the specified time and date, printed in

unaltered form, and not copied from the original printed page.

All of the pending claims -- namely claims 53-58 and 72-93 -- have been rejected as being anticipated by the U.S. Patent No. 4,013,894 to Foote et al. As the Examiner understands and appreciates, Foote et al. disclose a completely different type of "secure property document and system" than the present invention. However, applicant's claims, as originally presented, were sufficiently broad as to read on this document and system.

The patent to Foote et al. concerns an article, such as a credit card, which includes "two data sets": an optical data set and a magnetic data set. Each data set contains data elements having a spacial relationship to some of the data elements in the other data set.

Referring to Figures 1-3 of patent, the first data set is contained in a magnetic strip 18, whereas the second, optical data set comprises a number of "radiant energy modifying elements 20 which underlie the magnetic strip 18." (Col. 4, lines 25 and 26).

A reader (Fig. 4) reads and processes the data to determine whether or not the spacial relationship

corresponds to that which was previously recorded for this particular document.

Although the document (credit card) does contain embossed, visible alphanumeric characters 12 and 14 (Fig. 1) it is not suitable for recessing, nor do Foot et al. disclose or suggest that the document may receive, "document content comprising at least one of text and graphic images" applied "by a computer printer".

Accordingly, it is believed that independent claims 53, 72 and 88, as amended, are no longer anticipated by the Foote et al. patent.

This application is therefore believed to be in condition for immediate allowance. A formal Notice of Allowance is accordingly respectfully solicited.

Respectfully submitted,

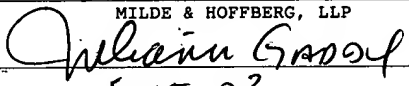
By


Karl F. Milde, Jr.

Reg. No. 24,822

MILDE & HOFFBERG, LLP
10 Bank Street - Suite 460
White Plains, NY 10606
(914) 949-3100

I hereby certify that this correspondence is being deposited with the United States Postal Services as first class mail in an envelope addressed to: Commissioner for Patent, P.O. Box 1450, Alexandria, VA 22313-1450
on 5-15-03


By Julian G. Gandy
Date 5-15-03

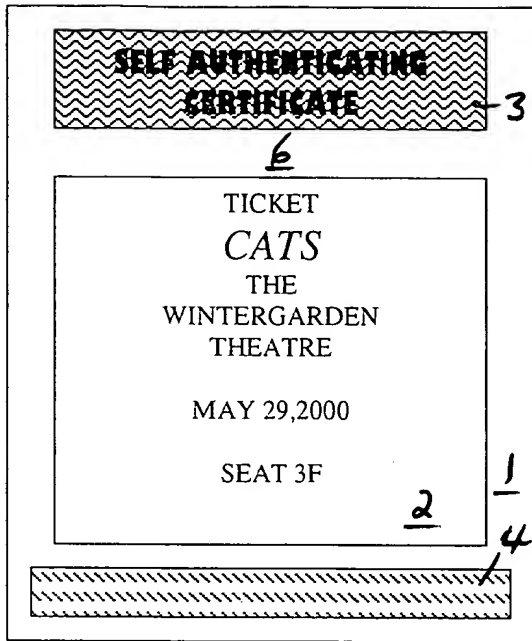


Fig. 1



Fig. 2

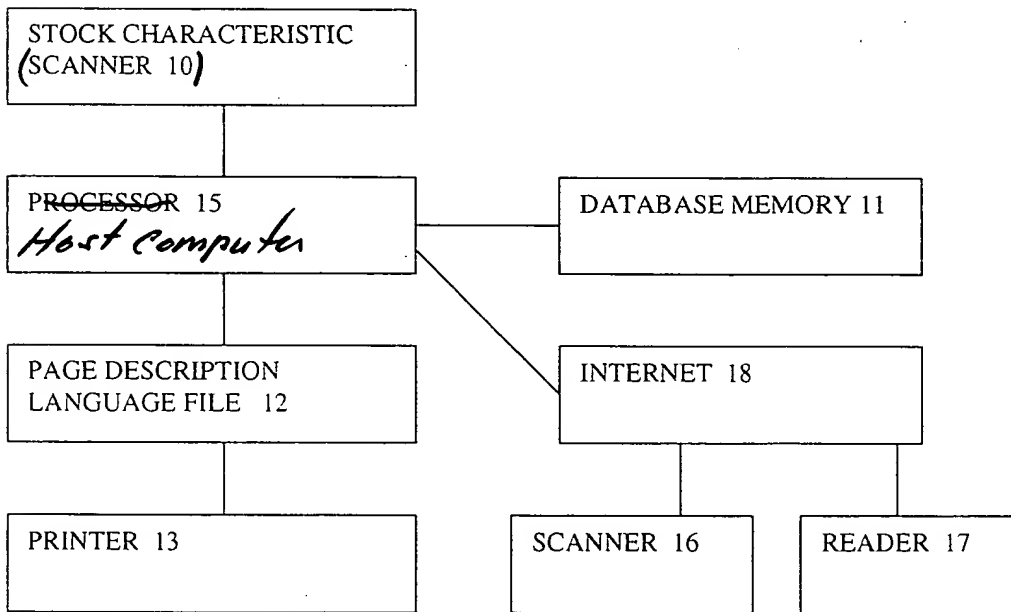


Fig. 3

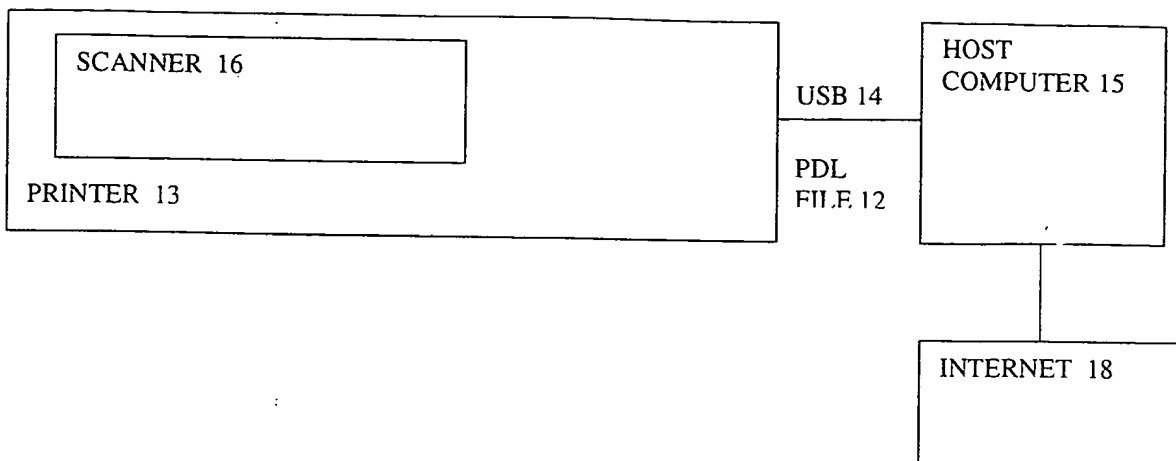


FIG. 4

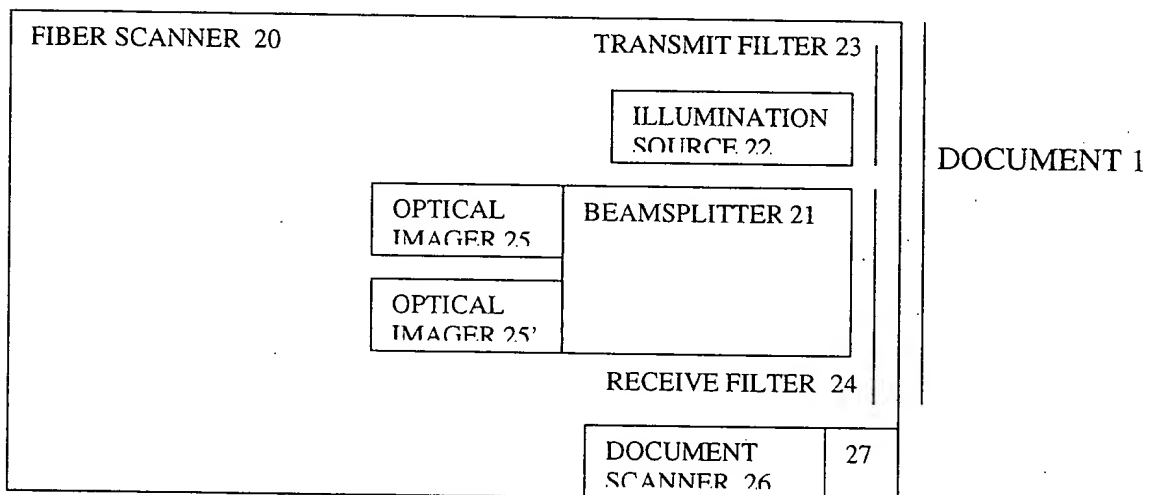


FIG. 5

Delete:
Processor 30

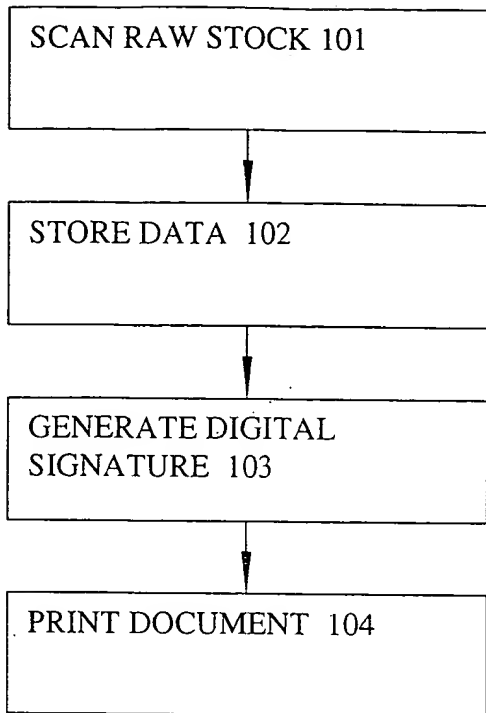
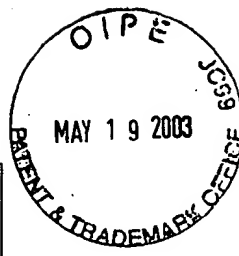


FIG. 6A

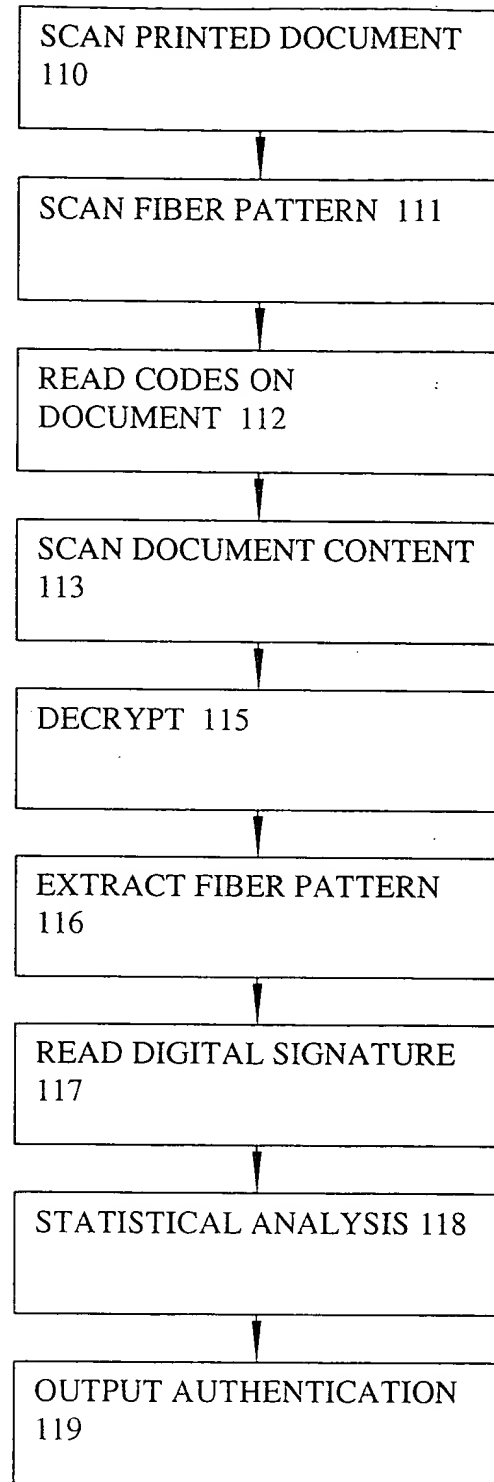


FIG. 6B